(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Numéro de publication : **0 440 549 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt : **91400201.9**

(51) Int. Cl.^{5} : **G07F 7/10**

(22) Date de dépôt : **29.01.91**

(30) Priorité : **30.01.90 FR 9001073**

(43) Date de publication de la demande :
07.08.91 Bulletin 91/32

(84) Etats contractants désignés :
DE ES FR GB IT NL

(71) Demandeur : **GEMPLUS CARD INTERNATIONAL**
avenue du Pic de Bertagne Parc d'activités de la Plaine de Jouques
F-13420 Gemenos (FR)

(72) Inventeur : **Le Roux, Jean-Yves**
Cabinet BALLOT-SCHMIT, 7, rue Le Sueur
F-75116 Paris (FR)

(74) Mandataire : **Schmit, Christian Norbert Marie et al**
Cabinet Ballot-Schmit 7, rue Le Sueur
F-75116 Paris (FR)

(54) Procédé et dispositif de gestion de transactions utilisant des cartes à microcircuit.

(57) Le procédé de gestion de transactions dans un système comportant des lecteurs de cartes et les cartes à microcircuit associées,consiste à organiser la mémoire des cartes destinée à l'enregistrement des transactions en deux zones, une zone accessible par présentation du code porteur à chaque transaction,pour les transactions de montant supérieur à une valeur prédéterminée, l'autre accessible pour les transactions de montant inférieur à la valeur prédéterminée, sans présentation systématique du code porteur : une présentation du code porteur commande l'écriture de bits d'ouverture d'espaces d'enregistrement dans cette deuxième zone jusqu'à ce que le nombre d'espaces ouverts soit égal à N prédéterminé.

L'invention s'applique, notamment aux cartes de crédit, aux cartes de téléphone, et aux cartes multiusages.

EP 0 440 549 A1

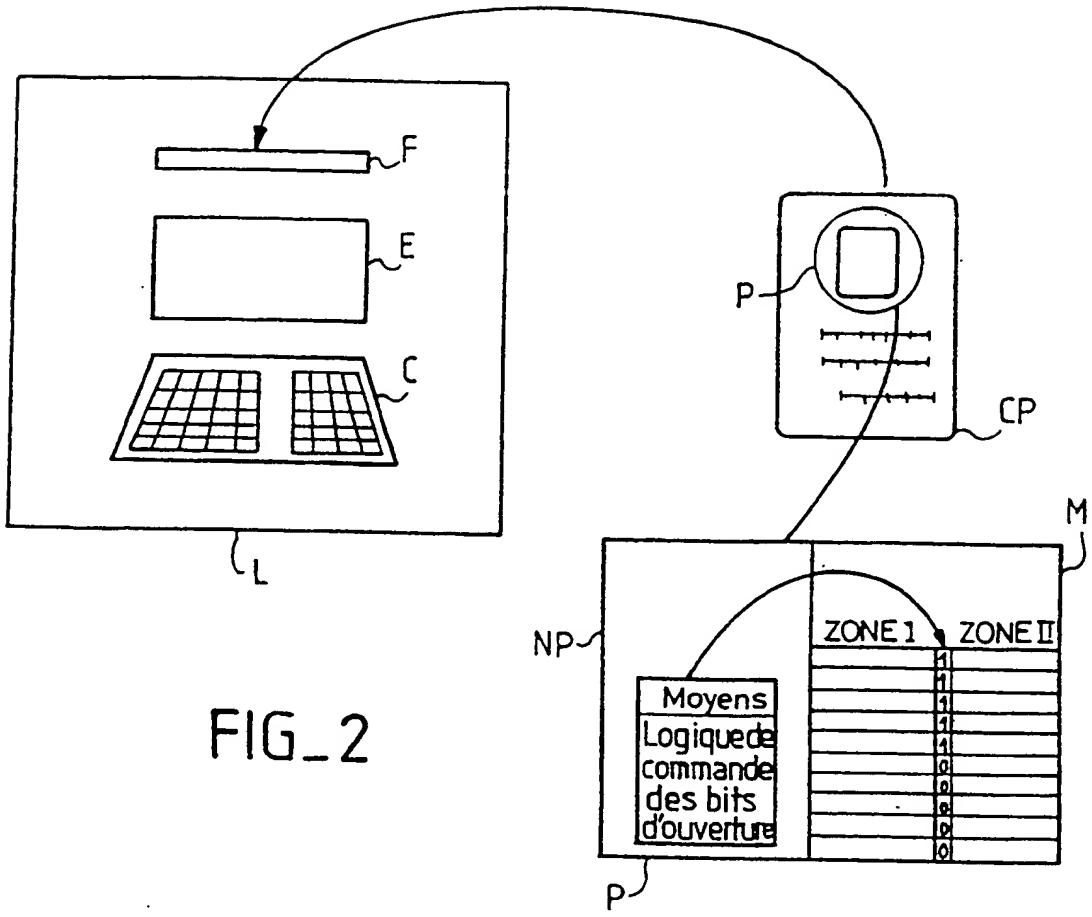


FIG_2

PROCEDE ET DISPOSITIF DE GESTION DE TRANSACTIONS UTILISANT DES CARTES A MICROCIRCUIT

L'invention se rapporte au domaine des systèmes de transactions utilisant des cartes à microcircuit, et plus particulièrement à un procédé, et au dispositif correspondant, de gestion de transactions utilisant de telles cartes.

Classiquement les cartes à microcircuit sont utilisées dans les systèmes de transactions bancaires, et, pour ce type de transactions, l'utilisation de la carte dans un lecteur nécessite la présentation à ce lecteur d'un code confidentiel propre au porteur, autorisant l'exécution de la transaction, dès que celle-ci met en jeu une somme d'argent. D'autres applications peuvent aussi ne pas nécessiter la présentation de ce code confidentiel, notamment si elles ne mettent pas en jeu le microcircuit et utilisent simplement la lecture d'une piste magnétique portée par la carte. Mais actuellement en général, dès que l'application requise utilise le microcircuit, notamment pour enregistrer une transaction dans un espace mémoire prévu à cet effet, la présentation du code du porteur est systématique, quel que soit le montant de la transaction.

Un tel système est parfaitement sécurisé, mais il présente évidemment l'inconvénient d'être lourd et d'utilisation un peu fastidieuse dès lors que le montant des transactions est faible : si l'on conçoit en effet de présenter son code confidentiel pour de gros montants, et que l'on apprécie la sécurité ainsi attachée à de telles transactions, la présentation systématique du code confidentiel pour les achats de faible montant parait disproportionnée par rapport au risque correspondant.

En conséquence pour les cartes multi-usages susceptibles d'être développées dans la période à venir, et notamment pour les cartes de crédits, cartes de téléphone etc...il convient de traiter de manières différentes les transactions impliquant des montants importants et celles qui ne mettent en jeu que de faibles montants.

L'invention a pour objet un procédé, et un dispositif correspondant, de gestion de transactions utilisant des cartes à microcircuit, permettant d'éviter la présentation systématique du code confidentiel par le porteur pour les transactions estimées au préalable d'enjeu faible, tout en maintenant une sécurité suffisante pour le porteur, et cela par des moyens suffisamment simples.

Selon l'invention, le procédé de gestion de transactions dans un système mettant en oeuvre des lecteurs de cartes et des cartes à microcircuit associées dont les porteurs sont reconnus par le système au moyen de codes porteurs confidentiels, caractérisé en ce qu'il consiste à organiser l'espace mémoire des cartes destiné à l'enregistrement des transactions en au moins une zone accessible sans présentation systématique du code porteur pour des transactions, une présentation du code, par un porteur commandant l'écriture de bits d'ouverture d'espaces d'enregistrement, dans cette zone, jusqu'à ce que le nombre d'espaces ouverts soit égal à un nombre prédéterminé N, N étant supérieur ou égal à 2.

L'invention a également pour objet un dispositif destiné à la mise en oeuvre de ce procédé.

L'invention sera mieux comprise et d'autres caractéristiques apparaîtront à l'aide de la description qui suit, faite au regard des figures annexées.

La figure 1 est l'organigramme d'un exemple du procédé de gestion selon l'invention.

La figure 2 illustre schématiquement le dispositif destiné à sa mise en oeuvre,selon l'invention ;.

Les figures 3a et 3b illustrent la zone mémoire utilisée pour les transactions de montants inférieurs à un seuil, respectivement avant et après présentation du code porteur.

Comme indiqué ci-dessus, le procédé selon l'invention est tel que la présentation du code confidentiel du porteur au lecteur de cartes donne la possibilité au porteur de bénéficier d'un nombre N de "droits" sans avoir à présenter son code à chaque "consommation" de ce droit N>=2 : par exemple le porteur peut bénéficier de N=5 transactions monétiques de montant inférieur à 100 F chacune après chaque présentation du code.

Pour cela, le microcircuit permet d'aiguiller l'enregistrement des transactions correspondantes (par exemple, les transactions inférieures à 100 F) vers une zone comportant un nombre fini d'espaces d'enregistrement de données, et le procédé selon l'invention prévoit, lors de la constitution de la carte à microcircuit un bit initialement à 0 en tête de chaque espace d'enregistrement et susceptible de changer de valeur pour signifier l'ouverture de l'espace d'enregistrement correspondant, sur commande programmée dans le microcircuit dès la constitution de la carte.

Cette commande actionnée par présentation du code porteur ouvre des espaces d'enregistrement non utilisés auparavant jusqu'à ce que le nombre d'espaces ouverts soit égal à N (5 par exemple).

Ainsi au moment de la première utilisation d'une carte neuve, le lecteur demande la composition du code confidentiel et, après réception de ce code et validation par le circuit, celui-ci transmet une commande qui d'une part permet d'accéder à la zone mémoire de transactions dite ZONE I ci-après, prévue pour les transactions de montant important, et d'autre part inverse les bits d'entête de N espaces d'enregistrements dans la zone mémoire de transactions dite ZONE II ci-après, prévue pour les transactions de fai-

ble montant, ce qui a pour effet d'ouvrir les droits correspondants à ces N espaces sans recomposer le code.

Si la transaction qui suit est une transaction de montant important, l'enregistrement a lieu dans la zone correspondante, et aucun des N espaces ouverts n'est consommé. Si la transaction est de faible montant l'enregistrement a lieu dans un des N espaces ouverts , et N-1 espaces restent disponibles pour les transactions de faible montant suivantes.

Lors de l'utilisation suivante, le code ne sera pas demandé au porteur, via le lecteur de cartes, tant que les transactions resteront de faible montant et que les espaces d'enregistrement ouverts ne seront pas tous utilisés.

Par contre, le code sera à nouveau demandé dès que le montant de la transaction sera important d'une part, ou, pour une transaction de faible montant, dès que tous les espaces ouverts auront été utilisés : dans ces deux cas la composition du code commandera l'ouverture d'espaces d'enregistrement dans la zone mémoire affectée aux transactions de faible montant, pour ouvrir N nouveaux espaces dans le second cas, lorsque espaces ouverts précédemment ont été épuisés.

La figure 1 illustre un exemple d'organigramme du procédé de gestion de transactions selon l'invention décrit ci-après.

Après la phase initiale, 1, d'insertion de la carte dans le lecteur et de demande de transaction via le clavier du lecteur, le lecteur demande la présentation du code, étape 3, si le montant de la transaction T demandée correspond à une valeur supérieure ou égale à une valeur de seuil prédéterminée S,lors d'un test, étape 2. Un test sur la valeur du code, étape 4, autorise l'enregistrement de la transaction en ZONE I, étape 5, si le code est correct et refuse la transaction (vers FIN) si le code n'est pas correct.

Le lecteur peut ne pas tenir compte de cette transaction enregistrée en ZONE I pour la gestion de la ZONE II et l'opération est alors terminée.

Dans le mode de réalisation, préféré correspondant à l'organigramme de la figure 1, la présentation correcte du code porteur ayant été effectuée, le lecteur commande la lecture des bits d'ouverture des N premiers espaces vides en ZONE II. Si n bits d'ouverture parmi les N lus sont à 1, alors par logique programmée à l'intérieur du microcircuit ou par logique câblée, les N-n bits suivants sont mis à 1. L'opération est alors terminée.

Lorsque la transaction demandée est de montant inférieur à S, lors du test de l'étape 2, le lecteur commande la lecture du bit d'ouverture du premier espace vide en ZONE II, étape 8, puis teste sa valeur, étape 9. Si le bit est à 1, l'enregistrement de la transaction a lieu immédiatement, étape 10,dans l'espace correspondant en ZONE II.

Par contre, si ce bit est encore à 0, le lecteur demande la composition du code porteur, étape 11, et vérifie s'il est correct, étape 12 : si non, la transaction est refusée, vers FIN, et si oui, le lecteur commande le lancement, par la logique interne de la carte, de l'écriture à 1 des bits d'ouverture des N premiers espaces vides en ZONE II, étape 13, puis l'enregistrement de la transaction, étape 10, dans le premier espace ouvert en ZONE II.

La figure 2 est un schéma du dispositif destiné à la mise en oeuvre du procédé décrit ci-dessus.Il comporte un lecteur L avec la fente F destinée à l'insertion d'une carte à microcircuit CP, son écran E et son clavier F pour le dialogue interactif entre le lecteur L et le porteur de la carte. Une carte CP comporte le microcircuit P et éventuellement des pistes magnétiques et/ou des inscriptions en clair. Le microcircuit P comporte le microprocesseur µP incluant sous forme d'un programme préenregistré et inaccessible des moyens logiques de commande des bits d'ouverture, et un espace mémoire associé M de type EPROM ou EEPROM non effaçable, comportant les zones I et II d'enregistrement des transactions comportant chacune des espaces d'enregistrement prédéfinis. Dans chaque espace d'enregistrement de la ZONE II est prévu en tête le bit d'ouverture initialement à 0 et susceptible d'être mis à 1 par commande interne du microcircuit.

Les figures 3a et 3b illustrent la zone mémoire II, respectivement avant présentation du code porteur, aucun espace n'étant accessible en écriture, et après présentation du code porteur suite à une demande de transaction de montant inférieur au seuil S, le premier espace ayant reçu l'enregistrement de la transaction correspondante dans un mode de réalisation où N a été choisi égal à 5 : 4 espaces restent disponibles en écriture sans présentation du code, les suivants restant inaccessibles en écriture.

L'avantage du procédé de gestion de transactions selon l'invention est que la sécurité attachée aux transactions reste la même que dans les systèmes antérieurs pour les transactions de montants importants par la présentation systématique du code porteur, mais que simultanément des transactions de montants faibles peuvent être effectuées en réduisant notablement le nombre de présentations du code porteur,sans toutefois laisser la zone correspondante complètement ouverte, cela afin d'éviter les fraudes, notamment en cas de perte ou vol de la carte : le montant correspondant à un fraude est au plus égal à N.S.

L'invention n'est pas limitée au mode de réalisation précisément décrit et représenté. En particulier, il est possible de prévoir une partition de la mémoire de la carte en un nombre de zones supérieur, par exemple 3, en prévoyant une deuxième valeur de seuil, par exemple S'<S, la présentation du code permettant l'ouverture d'un nombre d'espaces d'enregistrement plus grand dans la troisième zone par exemple N', mais pour des transactions de montants

faibles, inférieurs à S', la ZONE II étant alors réservée aux transactions de montants compris entre S et S'.

De plus, l'ordre des étapes dans l'organigramme de la figure 1 n'est donné qu'à titre d'exemple et comme indiqué ci-dessus les étapes 6 et 7 permettant de compléter à N le nombre d'espaces ouverts en ZONE II après présentation du code pour une transaction de montant élevé enregistrée en ZONE I peuvent être supprimées ou effectuées avant l'étape 5 de l'enregistrement en ZONE I.

Dans un autre perfectionnement, le nombre N est un nombre aléatoire valant 0 ou 1 selon le résultat d'un tirage. Ce tirage peut être organisé dans le lecteur, ou dans le programme de la carte, par un algorithme mis en oeuvre à cet effet, automatiquement par ce lecteur ou cette carte au moment de l'introduction de la carte dans ce lecteur. Quand le résultat du tirage est 0, on demande la composition du code secret, quand N vaut 1 on s'en passe. Ce mode peut bien entendu être couplé avec la fonctionnalité de seuil de dépense autorisé. C'est-à-dire ce tirage au sort ne concerne que les petites dépenses. Pour les grosses, il faut toujours indiquer le code secret au lecteur. Au lieu d'être aléatoire le tirage au sort peut aussi être pseudo-aléatoire si les algorithmes de tirage sont plus faciles à mettre en oeuvre dans l'espace mémoire réduit de la carte.

Revendications

1. Procédé de gestion de transactions dans un système mettant en oeuvre des lecteurs de cartes et des cartes à microcircuit associées dont les porteurs sont reconnus par le système au moyen de codes porteurs confidentiels, caractérisé en ce qu'il consiste à organiser l'espace mémoire des cartes destiné à l'enregistrement des transactions en au moins une zone accessible sans présentation systématique du code porteur pour des transactions, une présentation du code, par un porteur commandant l'écriture de bits d'ouverture d'espaces d'enregistrement, dans cette zone, jusqu'à ce que le nombre d'espaces ouverts soit égal à un nombre prédéterminé N, N étant supérieur ou égal à 2.

2. Procédé selon la revendication 1 dans lequel on organise l'espace mémoire des cartes en au moins deux zones distinctes, une première accessible pour un premier type de transaction, par présentation du code à chaque transaction, et une deuxième zone accessible pour un deuxième type de transactions, selon le mode de cette revendication 1, caractérisée en ce que les transactions sont orientées par le lecteur vers la première ou la deuxième zone mémoire des cartes à microcircuit selon que le montant qu'elles représentent est supérieur ou inférieur à une valeur de seuil prédéterminée.

3. Procédé selon la revendication 1 ou la revendication 2, caractérisé en ce que, après chaque demande de transaction et affichage de son montant, le lecteur de carte demande la composition du code lorsqu'il n'y a plus d'espaces d'enregistrement ouverts dans la zone correspondante, la composition du code dans ce cas commandant à nouveau l'écriture de N bits d'ouverture dans les N premiers espaces non enregistrés suivant ceux déjà utilisés dans cette zone.

4. Procédé selon la revendication 3, caractérisé en ce que la composition du code porteur faisant suite à une demande de transaction d'un montant supérieur au seuil, enregistrée dans la première zone mémoire, commande la lecture des bits d'ouverture des espaces non enregistrés suivant ceux déjà utilisés dans la seconde zone mémoire et l'écriture de ceux, jusqu'à N, non déjà écrits pour ouverture des espaces correspondants.

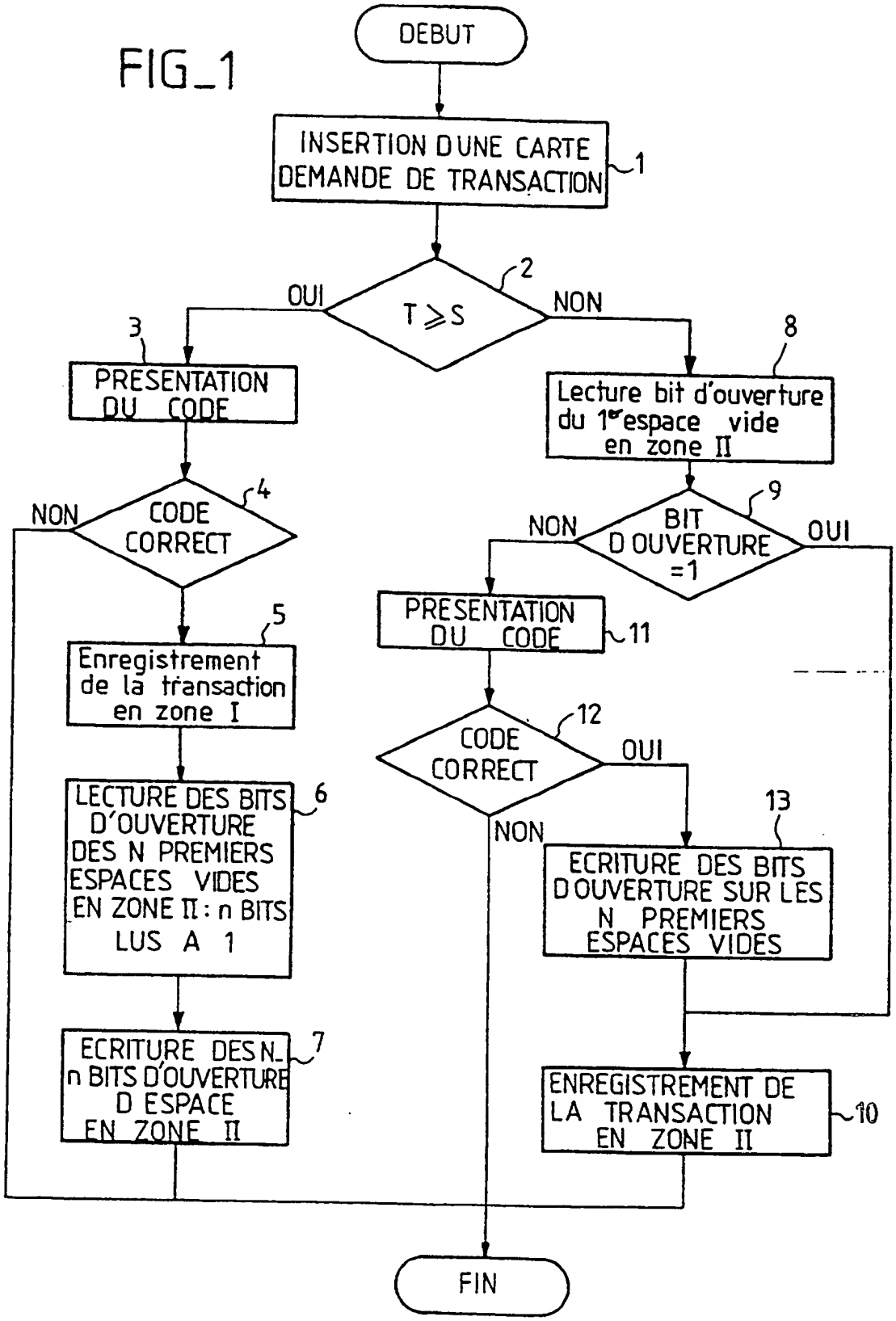
5. Dispositif de gestion de transactions destiné à la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce qu'il comporte, dans les cartes à microcircuit des moyens logiques inaccessibles commandant l'écriture des bits d'ouverture d'espaces d'enregistrement dans la deuxième zone mémoire, cette mémoire étant de type EPROM, ou EEPROM utilisée en EPROM, inscriptible et non effaçable.

6. Dispositif selon la revendication 5, caractérisé en ce que les moyens logiques de commande d'écriture des bits d'ouverture d'espaces d'enregistrement sont constitués d'un programme préenregistré dans le microcircuit.

7. Dispositif selon la revendication 5, caractérisé en ce que les moyens logiques de commande d'écriture des bits d'ouverture d'espaces d'enregistrement sont constitués d'un circuit logique.

8. Procédé de gestion de transactions dans un système mettant en oeuvre des lecteurs de cartes et des cartes à microcircuit associées dont les porteurs sont reconnus par le système au moyen de codes porteurs confidentiels, caractérisé en ce qu'il consiste à organiser l'espace mémoire des cartes destiné à l'enregistrement des transactions en au moins une zone accessible sans présentation systématique du code porteur pour des transactions, une présentation du code par un porteur étant rendue nécessaire selon le résultat d'un tirage au sort.

FIG_1



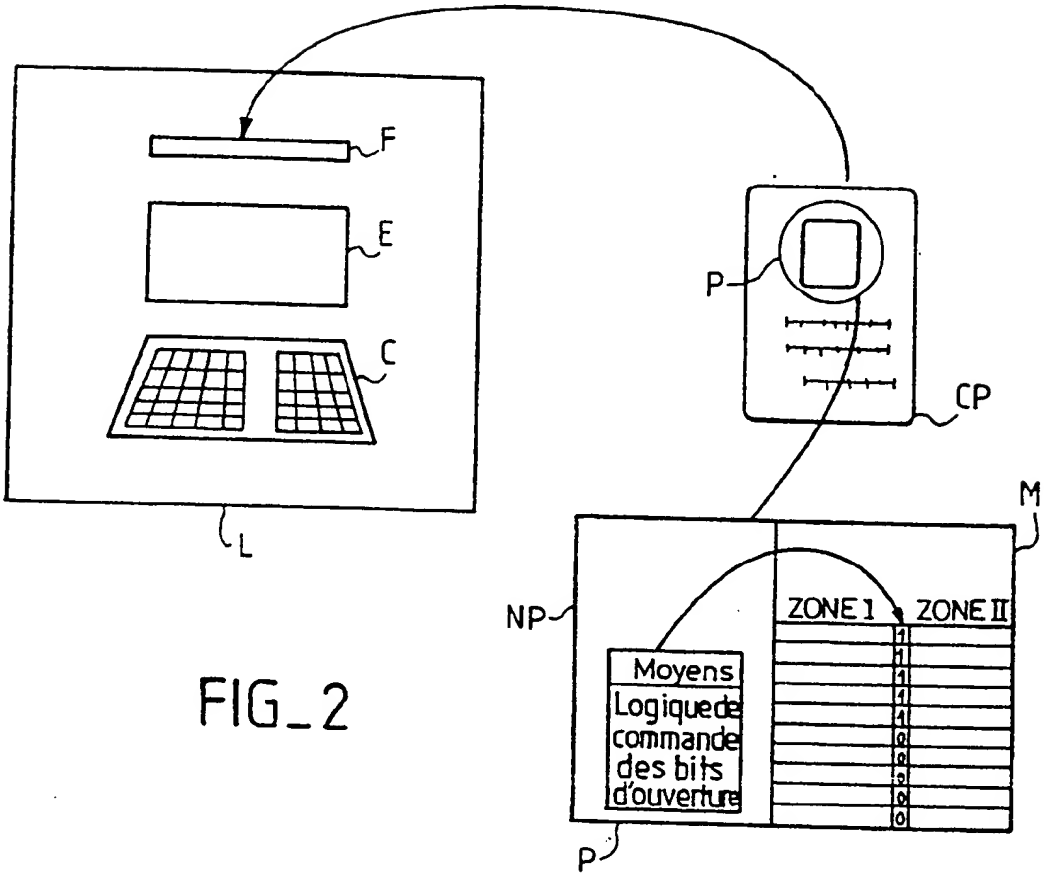


FIG_2

FIG_3-a

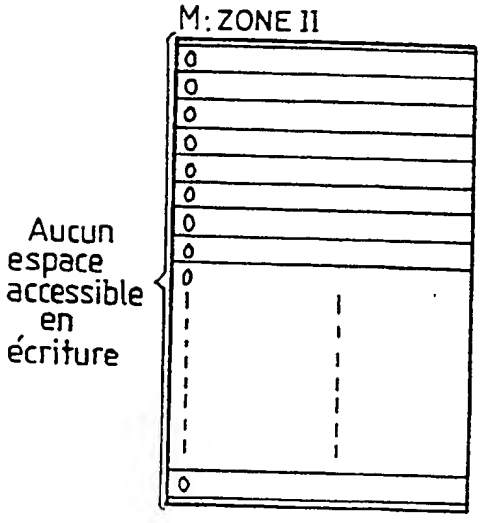


FIG_3-b